



EXPORT-IMPORT BANK OF THE UNITED STATES

[EXIM-OIG-2011-0010]

Office of Inspector General; Privacy Act of 1974; Systems of Records

AGENCY: The Export-Import Bank of the United States, Office of Inspector General

ACTION: Notice of New Privacy Act System of Records.

=====

SUMMARY: In accordance with the Privacy Act of 1974, the Export-Import Bank of the United States (hereafter known as "Ex-Im Bank"), Office of Inspector General (hereafter known as "OIG" or "Ex-Im Bank OIG") is giving notice of a new system of records entitled, "EIB-35-Office of Inspector General Investigative Records." The information in the new system of records will be used by the Ex-Im Bank OIG to conduct criminal, civil, and administrative investigations, and will contain identifying information about potential subjects, sources, and other individuals related to these investigations.

DATES: *Effective Date:* This system of records will become effective on June 15, 2012.

Comment Date: Comments should be received on or before (insert 30 days after publication in FR) to be assured of consideration.

ADDRESSES: You may submit comments, identified by Docket Number EIB-2011-0010 by one of the following methods:

1. Electronically through the eRulemaking Portal at <http://www.regulations.gov>. Please search for EIB-2011-0010.
2. By Mail/Hand Delivery/Courier: Alberto Rivera-Fournier, Ex-Im Bank, Office of Inspector General/811 Vermont Avenue, NW., Rm. 976, Washington, DC 20571. Please allow sufficient time for mailed comments to be received before the close of the comment period.

All comments received before the end of the comment period will be posted on <http://www.regulations.gov> for public

viewing. Hard copies of comments may also be obtained by writing to Counsel to the Inspector General, Ex-Im Bank, Office of Inspector General/811 Vermont Avenue, NW., Rm. 976, Washington, DC 20571.

FOR FURTHER INFORMATION CONTACT: Alberto Rivera-Fournier, Ex-Im Bank, Office of Inspector General, 811 Vermont Avenue, NW, Rm. 976, Washington, DC 20571 or by telephone (202) 565-3908 or facsimile (202) 565-3988.

SUPPLEMENTARY INFORMATION: Ex-Im Bank OIG is establishing a new system of records entitled "EIB-35-Office of Inspector General Investigative Records". The system of records is necessary for Ex-Im Bank OIG to carry out its investigative responsibilities pursuant to the Inspector General Act of 1978, as amended.

The Ex-Im Bank OIG was statutorily created in 2002 and organized in 2007. Ex-Im Bank OIG is statutorily directed to conduct and supervise investigations relating to programs and operations of Ex-Im Bank and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system are used in the course of investigating individuals and entities suspected of having committed illegal or unethical acts and in conducting related criminal prosecutions, civil proceedings, and administrative actions. The records may contain information about civil, criminal, or administrative wrongdoing, or about fraud, waste, mismanagement, or other violations of law or regulation. This information could be the basis for referrals to appropriate prosecutorial authorities for consideration of criminal or civil prosecution or Ex-Im Bank management for administrative action.

The collection and maintenance of records subject to this system is based on paper records and an electronic records management system, the "Inspector General Information System" (IGIS). IGIS allows the retrieval of records by name or other personal identifier. In accordance with 5 U.S.C. 552a(r), a report of this system of records has been provided to the Office of Management and Budget (OMB) and to the Congress. Concurrent with this system of records notice, Ex-Im Bank is proposing a rule to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. In addition, Ex-

Im Bank OIG is publishing a Privacy Impact Assessment of IGIS.

SYSTEM NAME: EIB-35-Office of Inspector General Investigative Records.

SECURITY CLASSIFICATION: The vast majority of the information in the system is Controlled Unclassified Information.

SYSTEM LOCATION: This system of records is located in the Ex-Im Bank OIG, 811 Vermont Avenue, NW, Washington, DC 20571.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Persons who are named individuals in investigations conducted by the Ex-Im Bank OIG.
2. Complainants and subjects of complaints collected through the Ex-Im Bank OIG Hotline or other sources.
3. Other individuals who have been identified as possibly relevant to, or who are contacted as part of an OIG investigation, including witnesses, confidential or non-confidential informants, and members of the general public who are named individuals in connection with investigations conducted by the Ex-Im Bank OIG.

CATEGORIES OF RECORDS IN THE SYSTEM: The system contains records related to complaints, and administrative, civil, and criminal investigations. These records include: a) Letters, memoranda, emails, and other documents citing complaints or alleged criminal, civil, or administrative misconduct. b) Investigative files which include reports of investigation with related exhibits, statements, affidavits, or records obtained during the investigation, information from subjects, targets, witnesses; material from governmental investigatory or law enforcement organizations (federal, state, local or international) and intelligence information; information of criminal, civil, or administrative referrals and/or results of investigations; public source materials; and reports and associated materials filed with Ex-Im Bank or other government agencies from, for example, exporters, lenders and other financial institutions, brokers, shippers, contractors, employers or other financial service providers.

Personal data in the system may consist of names, addresses, Social Security Numbers, fingerprints, physical identifying data, individual personnel and payroll information, and other evidence and background material existing in any form (i.e., photographs, reports, criminal histories, etc.).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: The Inspector General Act of 1978, as amended, 5 U.S.C. App. 3; 5 U.S.C. § 301; 44 U.S.C. § 3101.

PURPOSE(S): This system of records is established under the Inspector General Act of 1978, as amended, to maintain information and document OIG work related to investigations of criminal, civil, or administrative matters.

ROUTINE USES OF THESE RECORDS: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside Ex-Im Bank OIG as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- (A) To an appropriate Federal, State, territorial, tribal, local, or foreign law enforcement agency, licensing entity, or other appropriate authority charged with investigating, enforcing, prosecuting, or implementing a law (criminal, civil, administrative, or regulatory), where Ex-Im Bank OIG becomes aware of an indication of a violation or potential violation of such law or where required in response to compulsory legal process.
- (B) To Federal intelligence community agencies and other Federal agencies to further the mission of those agencies relating to persons who may pose a risk to homeland security.
- (C) To international governmental authorities in accordance with law and formal or informal international agreement;
- (D) To any individual or entity when necessary to elicit information that will assist an OIG investigation, inspection, or audit.
- (E) To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil or criminal

discovery or proceedings, litigation, and settlement negotiations.

- (F) To Federal, State, local, or foreign government entities or professional licensing authorities responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, or where Ex-Im Bank OIG becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation, or where Ex-Im Bank OIG has received a request for information that is relevant or necessary to the requesting entity's hiring or retention of an employee, or the issuance of a security clearance, license, contract, grant, or other benefit.
- (G) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records.
- (H) To the United States Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (i) Ex-Im Bank; (ii) any employee of Ex-Im Bank in his/her official capacity; (iii) any employee of Ex-Im Bank in his/her individual capacity where the Department of Justice or Ex-Im Bank has agreed to represent the employee; or, (iv) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation.
- (I) To third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation.
- (J) To a Member of Congress, or staff acting upon the Member's behalf, when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- (K) To an actual or potential party to litigation or the party's authorized representative for the purpose of negotiation or discussion of such matters as settlement, plea bargaining, or in informal discovery proceedings.
- (L) To the news media and the public, including disclosures pursuant to 28 CFR 50.2, unless it is determined that release of the specific information

in the context of a particular case would constitute an unwarranted invasion of personal privacy.

- (M) To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or of which they were a victim.
- (N) To appropriate agencies, entities, and persons when (1) the OIG suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the OIG has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the OIG or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the OIG's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.
- (O) To the National Archives and Records Administration or other Federal Government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
- (P) To appropriate persons engaged in conducting and reviewing internal and external peer reviews of the Ex-Im Bank OIG to ensure adequate internal safeguards and management procedures exist or to ensure that auditing standards applicable to Government audits are applied and followed.
- (Q) To the Council of Inspectors General on Integrity and Efficiency ("CIGIE") and other Offices of Inspectors General, as necessary, if the records respond to an audit, investigation, or review which is conducted pursuant to an authorizing law, rule or regulation, and in particular those conducted at the request of the CIGIE pursuant to 5 U.S.C. App. 3, § 11.
- (R) In an appropriate proceeding before a court, grand jury, or an administrative or adjudicative body, when the OIG determines that the records are arguably relevant to the proceeding; or in an

appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

- (S) To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an individual; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance or revocation of a grant or other benefit.
- (T) To federal, state, local, tribal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.
- (U) To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.

DISCLOSURE TO CONSUMER REPORTING AGENCIES: None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE: The records in this system are maintained in a variety of media, including paper, digital media (hard drives and magnetic tapes or discs), and an automated database. The records are maintained in limited access areas during duty hours and in locked offices at all other times.

RETRIEVABILITY: Paper media are retrieved numerically by investigation number. Electronic media are retrieved numerically by investigation number, by the name or identifying number for a complainant, subject, victim, or witness; by case number; by special agent, or other personal identifier.

SAFEGUARDS: All paper and electronic records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Ex-Im Bank facilities are protected from the outside by security personnel. Direct access to investigative records is restricted to authorized staff members of the OIG. Paper records, computers, and computer storage media are located

in controlled-access areas under supervision of program personnel. Manual records are in locked cabinets or in safes and can be accessed by key or combination formula only. Electronic records are protected by computer-logon identifications and password protection.

RETENTION AND DISPOSAL: OIG is in the process of developing a records retention schedule in conjunction with the National Archives and Records Administration (NARA). Closed files relating to a specific investigation are destroyed after ten years. Closed files containing information of an investigative nature but not relating to a specific investigation are destroyed after five years. Records existing on computer storage media are destroyed according to applicable OIG media sanitization practice.

SYSTEM MANAGER(S) AND ADDRESSES: The System Manager is the Inspector General, Ex-Im Bank OIG, 811 Vermont Avenue, NW, Rm. 976, Washington, DC 20571.

NOTIFICATION PROCEDURES: Pursuant to a concurrent notice of proposed rulemaking by Ex-Im Bank, this system of records will be generally exempt from the notice, access, and contest requirements of the Privacy Act. However, the Ex-Im Bank OIG will entertain written requests to the systems manager on a case-by-case basis for notification regarding whether this system of records contains information about an individual. Individuals seeking notification of any record contained in this system of records may submit a request in writing to the System Manager identified above. Individuals requesting notification must comply with the Ex-Im Bank Privacy Act regulations (12 CFR § 404.4).

RECORD ACCESS PROCEDURES: Same as "Notification Procedures'" above.

CONTESTING RECORD PROCEDURES: See "Notification procedures" and "Record access procedures" stated above.

RECORD SOURCE CATEGORIES: The information in this system of records is obtained from sources including, but not limited to, the individual record subjects; Ex-Im Bank officials and employees; employees of Federal, State, local, and foreign agencies; and other persons and entities; and public source materials.

EXEMPTIONS CLAIMED FOR THE SYSTEM: In general, the exemptions claimed are necessary in order to accomplish the law enforcement function of the OIG, to prevent subjects of investigations from frustrating the investigatory process, to prevent the disclosure of investigative techniques, to fulfill commitments made to protect the confidentiality of sources, to maintain access to sources of information, and to avoid endangering these sources and law enforcement personnel.

A. Pursuant to 5 U.S.C. § 552a(j)(2) and a proposed rulemaking by Ex-Im Bank, this system is proposed to be exempt from the following provisions of the Privacy Act: 5 U.S.C. §§ 552a (c)(3) and (4); (d)(1) through (4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f); and (g). The reasons for asserting such exemptions are the following:

(i) Disclosure to the individual named in the record pursuant to subsections (c)(3), (c)(4), or (d)(1) through (4) could seriously impede or compromise the investigation by alerting the target(s), subjecting a potential witness or witnesses to intimidation or improper influence, and leading to destruction of evidence. Disclosure could enable suspects to take action to prevent detection of criminal activities, conceal evidence, or escape prosecution.

(ii) Application of subsection (e)(1) is impractical because the relevance of specific information might be established only after considerable analysis and as the investigation progresses. Effective law enforcement requires the OIG to keep information that may not be relevant to a specific OIG investigation, but which may provide leads for appropriate law enforcement and to establish patterns of activity that might relate to the jurisdiction of the OIG and/or other agencies.

(iii) Application of subsection (e)(2) would be counterproductive to the performance of a criminal investigation because it would alert the individual to the existence of an investigation. In any investigation, it is necessary to obtain evidence from a variety of sources other than the subject of the investigation in order to verify the evidence necessary for successful litigation.

(iv) Application of subsection (e)(3) could discourage the free flow of information in a criminal law enforcement inquiry.

(v) Applications of subsections (e)(4)(G) and (H), and (f) would be counterproductive to the performance of a criminal investigation. To notify an individual at the individual's request of the existence of records in an investigative file pertaining to such individual, or to grant access to an investigative file could interfere with investigative and enforcement proceedings, deprive co-defendants of a right to a fair trial or other impartial adjudication, constitute an unwarranted invasion of personal privacy of others, disclose the identity or confidential sources, reveal confidential information supplied by these sources and disclose investigative techniques and procedures. Nevertheless, Ex-Im Bank OIG has published notice of its notification, access, and contest procedures because access may be appropriate in some cases.

(vi) Although the Office of Inspector General endeavors to maintain accurate records, application of subsection (e)(5) is impractical because maintaining only those records that are accurate, relevant, timely, and complete and that assure fairness in determination is contrary to established investigative techniques. Information that may initially appear inaccurate, irrelevant, untimely, or incomplete may, when collated and analyzed with other available information, become more pertinent as an investigation progresses.

(vii) Application of subsection (e)(8) could prematurely reveal an ongoing criminal investigation to the subject of the investigation.

(viii) The provisions of subsection (g) do not apply to this system if an exemption otherwise applies.

B. Pursuant to 5 U.S.C. §§ 552a (k)(2) and a proposed rulemaking by Ex-Im Bank, this system is proposed to be exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. §§ 552a (c)(3), (d)(1) through (4), (e)(1), (e)(4)(G), (e)(4)(H), and (f). These exemptions are claimed for the same reasons as stated in paragraph (a)(2) of this section, that is, because the system contains investigatory material compiled for law enforcement

purposes other than material within the scope of subsection 552a(j)(2). In addition, the reasons for asserting this exemption are because the disclosure and other requirements of the Privacy Act could substantially compromise the efficacy and integrity of the OIG operations. Disclosure could invade the privacy of other individuals and disclose their identity when they were expressly promised confidentiality. Disclosure could interfere with the integrity of information which would otherwise be subject to privileges (see, e.g., 5 U.S.C. § 552(b)(5)), and which could interfere with other important law enforcement concerns (see, e.g., 5 U.S.C. § 552(b)(7)).

C. Pursuant to 5 U.S.C. 552a(k)(5) and a proposed rulemaking by Ex-Im Bank, this system is proposed to be exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d)(1) through (4), (e)(1), (e)(4)(G) and (H), and (f). The reason for asserting this exemption is because the system contains investigatory material compiled for the purpose of determining eligibility or qualifications for federal civilian or contract employment.

Dated: May 1, 2012

Osvaldo L. Gratacos,
Inspector General

Sharon A. Whitt
Agency Clearance Officer
Billing Code 6690-01-P

[FR Doc. 2012-10897 Filed 05/04/2012 at 8:45 am;
Publication Date: 05/07/2012]